00/8119
ISR 31181
(3)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-282883
(43)Date of publication of application : 23.10.1998

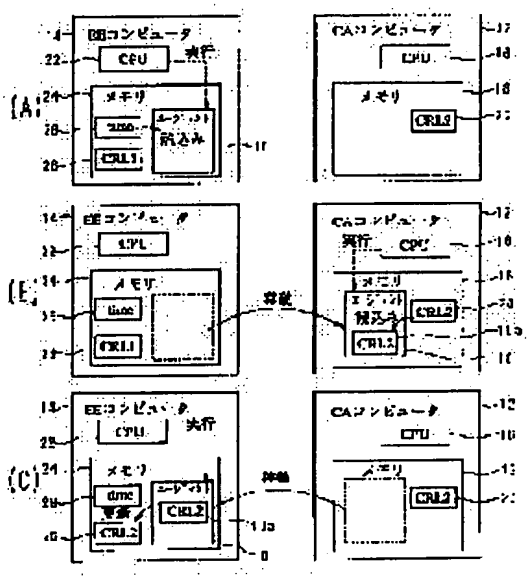
(51)Int.Cl. G09C 1/00
G06F 13/00
H04L 9/32

(21)Application number : 09-089774
(22)Date of filing : 08.04.1997

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : MORI TAKESHI

(54) METHOD FOR DISTRIBUTING INEFFECTIVE DIGITAL CERTIFICATE LIST

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the distributing method for CRL(ineffective digital certificate list) which can reduce the load of the designing of an application system and the system of an authentication office.
SOLUTION: An agent program 10 for a processing procedure for distributing CRL is used. This agent program 10 moves to the authentication office 12 according to its program. Then the latest CRL which is issued by the authentication office 12 is read in an authentication office memory 18. The agent program 10 moves to a terminal memory 24 together with the latest CRL according to its program. Then the CRL of a terminal entity 14 is updated into the latest CRL.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－282883

(43)公開日　平成10年(1998)10月23日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｅ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ

審査請求　未請求　請求項の数４　ＯＬ　（全 14 頁）

(21)出願番号　特願平9－89774

(22)出願日　平成９年(1997)４月８日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　森　健
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

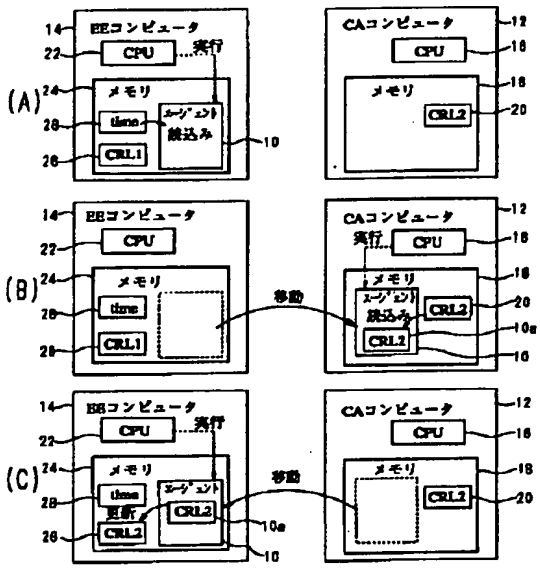
(74)代理人　弁理士　大垣　孝

(54)【発明の名称】　無効ディジタル証明書リストの配布方法

(57)【要約】

【課題】　アプリケーションシステムや認証局のシステムの設計の負荷を低減することができるＣＲＬの配布方法の提供。

【解決手段】　ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラム１０を用いる。このエージェントプログラム１０は、自身のプログラムに従って認証局１２へ移動する。次に、認証局メモリ１８に、認証局の発行している最新のＣＲＬを読み込む。一定時間の経過後に、エージェントプログラム１０は、自身のプログラムに従って、最新のＣＲＬを携えて、末端メモリ２４に移動する。そして、末端エンティティ１４のＣＲＬを最新のＣＲＬに更新する。



第１の実施の形態のブロック図

1

【特許請求の範囲】

【請求項１】　末端エンティティのコンピュータの記憶装置（以下、「末端メモリ」とも称する。）に、無効ディジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、

末端エンティティのコンピュータの中央演算装置（以下、「末端ＣＰＵ」とも称する。）によって、前記エージェントプログラムを起動し、

前記末端ＣＰＵによって前記エージェントプログラムを実行することにより、前記エージェントプログラムを認証局のコンピュータの記憶装置（以下「認証局メモリ」とも称する。）に格納し、

前記認証局のコンピュータの中央演算装置（以下、「認証局ＣＰＵ」とも称する。）によって前記エージェントプログラムを実行することにより、前記認証局メモリのうちの当該エージェントプログラムが使用するメモリ領域に、前記認証局の発行している最新の無効ディジタル証明書リストを格納し、かつ、一定時間の経過後に、前記エージェントプログラムを前記メモリ領域に格納された最新の無効ディジタル証明書リストと共に前記末端メモリに格納し、

前記末端ＣＰＵによって前記エージェントプログラムを実行することにより、前記末端メモリに格納されている無効ディジタル証明書リストを前記最新の無効ディジタル証明書リストに更新することを特徴とする無効ディジタル証明書リストの配布方法。

【請求項２】　請求項１に記載の無効ディジタル証明書リストの配布方法において、

前記一定時間を前記末端メモリに格納しておき、

前記エージェントプログラムが前記認証局のメモリに格納される前に、前記末端ＣＰＵによって前記エージェントプログラムを実行することにより、当該一定時間を前記末端メモリから当該エージェントプログラムに読込むことを特徴とする無効ディジタル証明書リストの配布方法。

【請求項３】　認証局のコンピュータの記憶装置（以下、「認証局メモリ」とも称する。）に、無効ディジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、

前記認証局のコンピュータの中央演算装置（以下、「認証局ＣＰＵ」とも称する。）によって、前記エージェントプログラムを起動し、

前記認証局ＣＰＵによって前記エージェントプログラムを実行することにより、前記認証局メモリのうちの当該エージェントプログラムが使用するメモリ領域に、前記認証局の発行している最新の無効ディジタル証明書リストを格納し、かつ、前記エージェントプログラムを前記メモリ領域に格納された最新の無効ディジタル証明書リストと共に末端エンティティのコンピュータの記憶装置（以下、「末端メモリ」とも称する。）に格納し、

2

前記末端エンティティのコンピュータの中央演算装置によって前記エージェントプログラムを実行することにより、当該末端メモリに格納されている無効ディジタル証明書リストを前記最新の無効ディジタル証明書リストに更新し、かつ、更新後に、前記エージェントプログラムを前記認証局メモリに格納することを特徴とする無効ディジタル証明書リストの配布方法。

【請求項４】　第１の認証局のコンピュータの記憶装置（以下、「第１認証局メモリ」とも称する。）に、無効ディジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、

前記第１の認証局のコンピュータの中央演算装置（以下、「第１認証局ＣＰＵ」とも称する。）によって、前記エージェントプログラムをそれぞれ起動し、

前記第１認証局ＣＰＵによって前記エージェントプログラムを実行することにより、前記第１認証局メモリのうちの該エージェントプログラムが使用するメモリ領域に、前記第１認証局の発行している最新の無効ディジタル証明書リストを格納し、かつ、前記エージェントプログラムを前記メモリ領域に格納された最新の無効ディジタル証明書リストと共に第２の認証局のコンピュータの記憶装置（以下、「第２認証局メモリ」とも称する。）に格納し、

前記第２の認証局のコンピュータの中央演算装置によって前記エージェントプログラムを実行することにより、当該第２認証局メモリに格納されている、前記第１認証局によって発行された無効ディジタル証明書リストを前記最新の無効ディジタル証明書リストに更新し、かつ、更新後に、前記エージェントプログラムを前記第１認証局メモリに格納することを特徴とする無効ディジタル証明書リストの配布方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＩＴＵ－Ｔ（国際電気通信連合　電気通信標準化部門）勧告Ｘ．５０９「ディレクトリー認証の枠組み」に準拠した認証局（証明書発行局（Certification Authority ；ＣＡ））が、無効となったディジタル証明書のリストを各ユーザ等の末端エンティティ（End Entity；ＥＥ）に配布するための方法に関する。

【０００２】

【従来の技術】インターネットのようなオープンネットワークシステムにおいて、例えば電子商取引（Electric Commerce;ＥＣ）といったシステムを実現するためには、ユーザの認証（身元保証）を行うこと、および、通信メッセージの機密性の確保および改竄の防止（正当性の保持）を行うことが不可欠である。このため、公開鍵暗号を利用した認証および暗号化方式の一例が、文献：「ソフトフエアデザイン、１９９６年１１月号、ｐｐ．

７２－８９」に「エレクトロニックコマースとセキュリティ」と題して記載されている。この方式においては、ユーザの認証のために、ディジタル証明書（電子印鑑証明書）が用いられる。このディジタル証明書は、ユーザの公開鍵を含み、その鍵が正しく当該ユーザの公開鍵であることを保証するものである。そして、このディジタル証明書は、ＩＴＵ－Ｔ勧告Ｘ．５０９に準拠した認証局によって発行される。

【０００３】

【発明が解決しようとする課題】認証局は、一定の有効期限が経過したり、証明書に関する鍵ペアの暗号が漏洩した等の理由によって、発行されたディジタル証明書を破棄または更新することにより無効とすることがある。そして、認証局は、上述のＩＴＵ－Ｔ勧告Ｘ．５０９に準拠した無効となったディジタル証明書のリスト（以下、「無効ディジタル証明書リスト」とも称し、「ＣＲＬ」とも表記する。）を作成して管理する必要がある。そして、このＣＲＬは、各ユーザに配布される必要がある。

【０００４】しかしながら、ＣＲＬの配布にあたり、次のような問題点がある。

【０００５】先ず、認証局（ＣＡ）から末端エンティティ（ＥＥ）へＣＲＬを配布するためには、オープンネットワークシステムにおいて実現されるアプリケーションシステムを設計する際に、ＣＲＬの配布を実現するためのメッセージやプロトコルといった仕組みを一緒に設計する必要がある。

【０００６】ところが、ＣＲＬを配布するための仕組みと、個々のアプリケーション（ＡＰ）システムとでは、設計のレベルが異なる。ここでレベルが異なるとは、アプリケーションシステムにおいては、個々のアプリケーションシステムに応じたメッセージやプロトコルといった仕組みを設計する必要がある（例えば、電子商取引のアプリケーションシステムにおいては、客、店および金融機関の間で、相手の確認や金銭のやり取りを行うためのメッセージやプロトコルを設計する必要がある。）のに対して、ＩＴＵ－Ｔ勧告Ｘ．５０９に準拠したＣＲＬを配布するための仕組みにおいては、個々のアプリケーションシステムの種類に依存しないより基本的なレベルでの仕組みを設計する必要があることをいう。

【０００７】このようにレベルが異なるため、ＣＲＬを配布するための仕組みの設計は、アプリケーションシステムを設計する上で大きな負担となる。

【０００８】また、ＣＲＬの内容は、認証局において運用上定められた一定時間毎に更新される。一方、ＣＲＬの配布の時間間隔は、アプリケーションシステムによって異なる。その結果、末端エンティティが保持しているＣＲＬと、認証局が保持している最新のＣＲＬとの間に時間的なずれが生じる。そして、更新および配布の時間間隔の設定が悪い場合には、この時間的なずれが大きくなる。その場合、末端エンティティが保持しているＣＲＬの信頼度が低下してしまう。このため、ＣＲＬの信頼度の低下を防ぐためには、ＣＲＬの更新の時間間隔に対するＣＲＬの配布の時間間隔を最適に設定することが求められる。

【０００９】ところが、アプリケーションシステムの設計に、ＣＲＬの配布の仕組みが組み込まれている場合には、ＣＲＬの配布の時間間隔を簡単には変更できない。ここで、ＣＲＬの配布の仕組みが組み込まれている場合とは、例えば、個々のアプリケーションシステムに応じたメッセージのやり取りと同時にＣＲＬの配布を行うように設計してある場合である。より具体的な例としては、電子商取引において店から金融機関への送金を行うのと同時にＣＲＬの配布を行うように設計してあるような場合である。この場合、送金が１日に１回だけの場合（通信費を節約したい場合や、夜間に１回、その日の売上を金融機関に送れば送金頻度が十分な場合が考えられる。）には、ＣＲＬの配布も１日に１回だけとなる。そして、店が客の身元をより正確に確認するためにより頻繁なＣＲＬの配布を希望しても、送金頻度を変更せずにＣＲＬの配布の時間間隔だけを後から変更することは困難である。

【００１０】また、複数の認証局（ＣＡ）どうしが協調して動作する、より大きなシステムを構築する場合には、認証局どうしの間で互いにＣＲＬを配布し合う仕組みが必要となる。ここで、認証局どうしが協調して動作するとは、互いに異なる認証局がそれぞれ発行したデジタル証明書を、互いに信用して良いという取り決めをしている場合をいう。このように、認証局どうしが協調して動作すれば、互いに異なる認証局によってそれぞれ認証（身元保証）された末端エンティティのユーザどうしが、互いに相手を信用することができる。これに対して、認証局が協調して動作しない場合には、互いに異なる認証局からディジタル証明書を付与された末端エンティティのユーザどうしは、通常、相手のディジタル証明書を信用することができない。

【００１１】ところが、既に一つの認証局が稼働しているシステムに、後から他の認証局からのＣＲＬの配布の仕組みを組み入れるためには、システムの設計を大きく変更する必要がある。このため、複数の認証局どうしを後から協調して動作させることは、システムの設計の上で大きな負担となる。

【００１２】このため、アプリケーションシステムや認証局のシステムの設計の負荷を低減することができる新規なＣＲＬの配布方法の実現が望まれていた。

【００１３】

【課題を解決するための手段】そこで、この出願に係る発明者は、種々の検討を重ねた結果、アプリケーションシステムや認証局のシステム自体に無効ディジタル証明書リスト（ＣＲＬ）の配布の仕組みを設計するのではな

く、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラムを用いることを考えついた。

【００１４】［第１の無効ディジタル証明書リストの配布方法について］この発明の第１の無効ディジタル証明書リスト（ＣＲＬ）の配布方法によれば、末端エンティティのコンピュータの記憶装置（末端メモリ）に、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、末端エンティティのコンピュータの中央演算装置（末端ＣＰＵ）によって、エージェントプログラムを起動し、末端ＣＰＵによってエージェントプログラムを実行することにより、エージェントプログラムを認証局のコンピュータの記憶装置（認証局メモリ）に格納し、認証局のコンピュータの中央演算装置（認証局ＣＰＵ）によってエージェントプログラムを実行することにより、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新のＣＲＬを格納し、かつ、一定時間の経過後に、エージェントプログラムをメモリ領域に格納された最新のＣＲＬと共に末端メモリに格納し、末端ＣＰＵによってエージェントプログラムを実行することにより、末端メモリに格納されているＣＲＬを最新のＣＲＬに更新することを特徴とする。

【００１５】このように、この発明の第１の無効ディジタル証明書の配布方法によれば、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラムを用いる。

【００１６】そして、第１の無効ディジタル証明書リストの配布方法によれば、ＣＲＬの配布を行うにあたり、先ず、末端メモリに格納されていたエージェントプログラムを末端ＣＰＵによって起動する。すなわち、末端ＣＰＵによってエージェントプログラムの実行を開始する。

【００１７】次に、末端ＣＰＵによってエージェントプログラムを実行することにより、エージェントプログラム自身は、認証局メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って認証局へ移動する。

【００１８】次に、認証局メモリに格納されたエージェントプログラムは、認証局ＣＰＵによって実行される。その結果、エージェントプログラムの処理手順に従って、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新のＣＲＬが格納される。

【００１９】そして、エージェントプログラムは、一定時間、認証局メモリに格納されている。すなわち、エージェントプログラムは、一定時間、認証局に駐在する。また、エージェントプログラムが認証局に駐在している間に認証局のＣＲＬが更新された場合には、更新されたＣＲＬが最新のＣＲＬとなるが、エージェントプログラムでＣＲＬの更新を監視し、この更新されたＣＲＬをメモリ領域に新たに格納する。

【００２０】そして、一定時間の経過後に、エージェントプログラムは、メモリ領域に格納された最新のＣＲＬと共に末端メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って、最新のＣＲＬを携えて、末端メモリに移動する。

【００２１】次に、末端メモリに格納されたエージェントプログラムは、末端ＣＰＵによって実行される。その結果、エージェントプログラムの処理手順に従って、末端メモリに格納されている古いＣＲＬは、戻ったエージェントプログラムが持ち帰った最新のＣＲＬに更新される。このようにして、エージェントプログラムにより認証局から末端エンティティへＣＲＬが配布される。

【００２２】このように、この発明の第１の無効ディジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにＣＲＬの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をＣＲＬの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【００２３】また、この発明の第１の無効ディジタル証明書リストの配布方法を実施するにあたり、好ましくは、一定時間を末端メモリに格納しておき、エージェントプログラムが認証局のメモリに格納される前に、末端ＣＰＵによってエージェントプログラムを実行することにより、この一定時間を末端メモリから当該エージェントプログラムに読込むと良い。

【００２４】このように、末端メモリに格納しておいた一定時間をエージェントプログラムに読み込ませて設定すれば、末端メモリに所望の値の一定時間を格納しておくことにより、エージェントプログラムが認証局に駐在している時間の長さを所望の長さとすることができる。その結果、エージェントプログラムが認証局から末端エンティティに戻ってくるタイミングを所望のタイミングとすることができる。このため、ＣＲＬの配布による末端エンティティのＣＲＬの更新のタイミングを所望のタイミングとすることができる。

【００２５】［第２の無効ディジタル証明書リストの配布方法について］ところで、第１の無効ディジタル証明書リストの配布方法によれば、エージェントプログラムが、一定時間、認証局に駐在する。そして、駐在している間、エージェントプログラムは、認証局のコンピュータの中央演算装置（認証局ＣＰＵ）によって実行される。また、エージェントプログラムは、認証局に駐在している間、認証局のコンピュータの記憶装置（認証局メモリ）の記憶容量のうちの一部分のメモリ領域を占有している。このため、認証局にエージェントプログラムが

駐在している間、認証局のコンピュータの負担が大きくなる。

【００２６】ところが、認証局のコンピュータの演算能力および記憶容量といった処理能力は、一般に、余裕が少ない。その上、多数の末端エンティティから多数のエージェントプログラムが認証局に駐在すると、認証局のコンピュータの負担が非常に大きくなる。その結果、認証局自身の処理が滞るおそれがある。例えば、認証局によるＣＲＬの発行に時間がかかってしまうおそれがある。

【００２７】そこで、認証局のコンピュータの負担の増大を抑制するため、この発明の第２の無効ディジタル証明書リストの配布方法よれば、認証局のコンピュータの記憶装置（認証局メモリ）に、無効ディジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、認証局のコンピュータの中央演算装置（認証局ＣＰＵ）によって、エージェントプログラムを起動し、認証局ＣＰＵによってエージェントプログラムを実行することにより、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新の無効ディジタル証明書リストを格納し、かつ、エージェントプログラムをメモリ領域に格納された最新の無効ディジタル証明書リストと共に末端エンティティのコンピュータの記憶装置（末端メモリ）に格納し、末端エンティティのコンピュータの中央演算装置（以下、「末端ＣＰＵ」とも称する。）によってエージェントプログラムを実行することにより、当該末端メモリに格納されている無効ディジタル証明書リストを最新の無効ディジタル証明書リストに更新し、かつ、更新後に、エージェントプログラムを認証局メモリに格納することを特徴とする。

【００２８】このように、この発明の第２の無効ディジタル証明書の配布方法によれば、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラムを用いる。

【００２９】そして、第２の無効ディジタル証明書リストの配布方法によれば、ＣＲＬの配布を行うにあたり、先ず、認証局メモリに格納されていたエージェントプログラムを認証局ＣＰＵによって起動する。すなわち、認証局ＣＰＵによってエージェントプログラムの実行を開始する。

【００３０】次に、認証局ＣＰＵによってエージェントプログラムを実行することにより、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新の無効ディジタル証明書リストが格納される。

【００３１】そして、エージェントプログラム自身は、メモリ領域に格納された最新の無効ディジタル証明書リストと共に、オープンネットワークシステムを介して送られて末端メモリに格納される。すなわち、エージェントプログラムは、自身のプログラムに従って末端エンティティへ移動する。

【００３２】次に、末端メモリに格納されたエージェントプログラムは、末端ＣＰＵによって実行される。その結果、エージェントプログラムの処理手順に従って、当該末端メモリに格納されている古い無効ディジタル証明書リストは、最新の無効ディジタル証明書リストに更新される。このようにして、エージェントプログラムにより認証局から末端エンティティへＣＲＬが配布される。

【００３３】そして、ＣＲＬの更新後に、エージェントプログラムは、認証局メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って、認証局メモリに移動する。

【００３４】このように、この発明の第２の無効ディジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにＣＲＬの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をＣＲＬの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【００３５】さらに、この発明の第２の無効ディジタル証明書リストの配布方法によれば、認証局ＣＰＵによって、エージェントプログラムを起動して、エージェントプログラムを末端メモリへ移動させる。このため、第２の無効ディジタル証明書リストの配布方法によれば、認証局へ末端エンティティからエージェントプログラムが殺到することがない。その結果、認証局のコンピュータの負担の増大を抑制することができる。従って、第２の無効ディジタル証明書リストの配布方法は、特に認証局のコンピュータの処理能力に余裕がない場合に適用して好適である。

【００３６】［第３の無効ディジタル証明書リストの配布方法について］また、複数の認証局が協調して動作するシステムを構築する場合には、複数の認証局がそれぞれ発行したＣＲＬを互いに配布する仕組みが必要となる。しかし、既存の認証局どうしを、後から協調して動作させるためには、従来は、システムの大きな変更が必要であった。

【００３７】そこで、認証局のシステムを大きく変更せずに、認証局どうしを協調して動作させるために、この発明の第３の無効ディジタル証明書リストの配布方法によれば、第１の認証局のコンピュータの記憶装置（以下、「第１認証局メモリ」とも称する。）に、無効ディジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、第１の認証局のコンピュータの中央演算装置（以下、「第１認証局ＣＰＵ」とも称する。）によって、エージェントプログラムをそれぞれ起動し、第１認証局ＣＰＵによ

ってエージェントプログラムを実行することにより、第１認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、第１認証局の発行している最新の無効ディジタル証明書リストを格納し、かつ、エージェントプログラムをメモリ領域に格納された最新の無効ディジタル証明書リストと共に第２の認証局のコンピュータの記憶装置（以下、「第２認証局メモリ」とも称する。）に格納し、第２の認証局のコンピュータの中央演算装置（以下、「第２認証局ＣＰＵ」とも称する。）によってエージェントプログラムを実行することにより、当該第２認証局メモリに格納されている、第１認証局によって以前に発行された無効ディジタル証明書リストを最新の無効ディジタル証明書リストに更新し、かつ、更新後に、エージェントプログラムを第１認証局メモリに格納することを特徴とする。

【００３８】このように、この発明の第３の無効ディジタル証明書リストの配布方法によれば、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラムを用いる。

【００３９】そして、第３の無効ディジタル証明書リストの配布方法によれば、第１認証局から第２認証局へＣＲＬの配布を行うにあたり、先ず、第１認証局メモリに格納されていたエージェントプログラムを第１認証局ＣＰＵによって起動する。すなわち、第１認証局ＣＰＵによってエージェントプログラムの実行を開始する。

【００４０】次に、第１認証局ＣＰＵによってエージェントプログラムを実行することにより、第１認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、第１認証局の発行している最新の無効ディジタル証明書リストが格納される。

【００４１】そして、エージェントプログラム自身は、メモリ領域に格納された最新の無効ディジタル証明書リストと共に、オープンネットワークシステムを介して送られて第２認証局メモリに格納される。すなわち、エージェントプログラムは、自身のプログラムに従って第２認証局へ移動する。

【００４２】次に、第２認証局メモリに格納されたエージェントプログラムは、第２認証局ＣＰＵによって実行される。その結果、エージェントプログラムの処理手順に従って、当該第２認証局メモリに格納されている、第１認証局によって以前に発行された古い無効ディジタル証明書リストは、最新の無効ディジタル証明書リストに更新される。このようにして、エージェントプログラムにより第１認証局から第２認証局へＣＲＬが配布される。

【００４３】そして、ＣＲＬの更新後に、エージェントプログラムは、第１認証局メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って、第１認証局メモリに移動する。

【００４４】このように、この発明の第３の無効ディジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにＣＲＬの配布の仕組みの処理手順を設計する。その結果、個々の認証局のシステムの設計をＣＲＬの配布の仕組みの設計から切り離して行うことができる。このため、認証局のシステムの設計の負担を軽減することができる。

【００４５】また、第２認証局から第１認証局へＣＲＬを配布する場合も、第１認証局から第２認証局へＣＲＬを配布する場合と同様にしてＣＲＬを配布することができる。さらに、第１認証局から第２認証局へＣＲＬを配布する場合の処理手順を繰返すことによって、３つ以上の認証局どうしの間でＣＲＬを互いに配布することも可能である。

【００４６】

【発明の実施の形態】以下、図を参照して、この発明の第１～第３の無効ディジタル証明書リストの配布方法の例についてそれぞれ説明する。

【００４７】［第１の実施の形態］第１の実施の形態では、図１および図２を参照して、この発明の第１の無効ディジタル証明書リスト（ＣＲＬ）の配布方法の一例について説明する。

【００４８】図１の（Ａ）～（Ｃ）は、第１の実施の形態のＣＲＬの配布方法の説明に供するブロック図である。また、図２は、第１の実施の形態のＣＲＬの配布方法の説明に供するフローチャートである。

【００４９】先ず、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラム（以下、単に「エージェント」とも称する。）１０が稼働する環境について説明する。通常は、認証局から多数の末端エンティティへＣＲＬが配布されるが、ここでは、１つの末端エンティティおよび認証局に注目してＣＲＬの配布方法について説明する。

【００５０】図１に、認証局のコンピュータ（「ＣＡコンピュータ」または「認証局」とも表記する。）１２と、末端エンティティのコンピュータ（「ＥＥコンピュータ」または「末端エンティティ」とも称する。）１４を示す。認証局１２と末端エンティティ１４とは、互いにオープンネットワークシステムによって接続してある。また、認証局１２および末端エンティティ１４は、いずれも、エージェント１０が動作可能な環境を有している。動作可能な環境とは、例えば、認証局１２と末端エンティティ１４との間でエージェント１０の受渡が可能な状態をいう。

【００５１】また、認証局１２は、認証局ＣＰＵ１６および認証局メモリ１８を具えている。この認証局メモリ１８には、この認証局が発行した最新の無効ディジタル証明書リスト（ＣＲＬ）が第１ＣＲＬファイル２０として格納されている。第１の実施の形態においては、第１

ＣＲＬファイル２０に、最新のＣＲＬとして「ＣＲＬ２」を格納してある。

【００５２】また、末端エンティティ１４は、末端ＣＰＵ２２および末端メモリ２４を具えている。この末端メモリ２４には、認証局から配布されたＣＲＬを格納するための第２ＣＲＬファイル２６が格納されている。ここでは、第２ＣＲＬファイルに、以前に認証局１２から配布された「ＣＲＬ１」を古いＣＲＬとして格納してある（図１の（Ａ））。

【００５３】尚、第２ＣＲＬファイル２６の内容が、第１ＣＲＬファイル２０の内容と同じ場合もあり得る。また、末端メモリ２４には、エージェントを認証局に駐在させる一定時間を設定したファイル２８が格納してある。

【００５４】そして、末端メモリ２４には、エージェントプログラム１０がコンパイルされた状態で格納してある（図１の（Ａ））。

【００５５】尚、ここでは、認証局メモリ１８や末端メモリ２４といったコンピュータの記憶装置は、コンピュータに内蔵されているものに限定する必要はなく、例えば、コンピュータに接続された外部記憶装置、例えば、ハードディスク装置を用いても良い。

【００５６】次に、第１の実施の形態におけるＣＲＬの配布方法について説明する。

【００５７】ＣＲＬの配布を行うにあたり、先ず、末端メモリ２４に格納されていたエージェント１０を末端ＣＰＵ２２によって起動する（図２のＳ１）。すなわち、末端ＣＰＵ２２によってエージェントプログラム１０の実行を開始する。起動にあたっては、例えば、末端メモリ２４中に格納されているローカルな関数の呼び出しを末端ＣＰＵ２２によって行うことによって、エージェント１０の実行を開始させると良い。

【００５８】次に、末端ＣＰＵ２２によってエージェントプログラム１０を実行することにより、当該エージェントプログラム１０に一定時間を読み込む（図２のＳ２）。一定時間の読込みにあたっては、末端メモリ２４に格納しておいた一定時間を設定したファイル２８に格納された一定時間をエージェントプログラム１０に読み込む。すなわち、エージェントプログラム１０は、起動されると、先ずファイル２８に格納した一定時間を読込むようプログラムされている。

【００５９】従って、このファイル２８に、所望の値の一定時間（例えば、何分、何時間もしくは何日間という設定）を格納しておくことにより、エージェントプログラムが認証局１２に駐在している時間の長さを所望の長さとすることができる。その結果、エージェントプログラム１０が認証局１２から末端エンティティ１４に戻ってくるタイミングを所望のタイミングとすることができる。このため、ＣＲＬの更新を所望のタイミングで行なうことができる。

【００６０】次に、末端ＣＰＵ２２によってエージェントプログラム１０を実行することにより、エージェントプログラム１０自身は、認証局１２にオープンネットワークシステムを介して送られて、認証局メモリ１８に格納される（図１の（Ｂ））。すなわち、エージェントプログラム１０は、自身のプログラムに従って認証局メモリ（ＣＡメモリ）１８へ移動する（図２のＳ３）。

【００６１】次に、認証局ＣＰＵ１６によってエージェントプログラム１０を実行することにより、認証局メモリ１８のうちのこのエージェントプログラム１０が使用するメモリ領域に、認証局の発行している最新のＣＲＬを格納する（図１の（Ｂ））。ここでは、このメモリ領域のＣＲＬ読込みファイル１０ａに、第１ＣＲＬファイル２０から最新ＣＲＬとして「ＣＲＬ２」を読み込む（図２のＳ４）。尚、図１の（Ｂ）においては、エージェント１０のＣＲＬ読込みファイル１０ａに「ＣＲＬ２」が読込まれた状態を示す。

【００６２】次に、エージェントプログラム１０は、一定時間、認証局メモリ１８に駐在する。駐在している間、認証局ＣＰＵ１６によって、エージェントプログラム１０を実行することにより、経過時間を計測する。また、駐在している間、認証局ＣＰＵ１６によって、エージェントプログラム１０を実行することにより、第１ＣＲＬファイル２０の内容の更新状況を監視する。監視にあたっては、例えば、第１ＣＲＬファイル２０のファイルの更新日時やファイルのバージョンを調べるようにすると良い。そして、駐在している間に最新ＣＲＬ２０の内容が更新された場合は、更新された新しいＣＲＬをＣＲＬ読込みファイル１０ａに読込む（図２のＳ５）。

【００６３】また、図２において、太線の枠で示したＳ５およびＳ６のステップの処理は、認証局ＣＰＵ１６がエージェントプログラム１０を実行することによって行われる。また、Ｓ５およびＳ６のステップ以外の処理（細線の枠で示されたステップＳ１～Ｓ４およびＳ７）の処理は、末端ＣＰＵ２２がエージェントプログラム１０を実行することによって行われる。

【００６４】次に、認証局ＣＰＵ１６によってエージェントプログラム１０を実行することにより、一定時間の経過後に、エージェントプログラム１０をメモリ領域に格納された第１ＣＲＬファイル２０（その内容は「ＣＲＬ２」である。）と共に、オープンネットワークシステムを介して送って末端メモリ２４に格納する（図１の（Ｃ））。すなわち、エージェントプログラム１０は、自身のプログラムに従って、ＣＲＬ読込みファイル１０ａを携えて、末端メモリ（ＥＥメモリ）２４に移動する（図２のＳ６）。

【００６５】次に、末端メモリ２４に格納されたエージェントプログラム１０は、末端ＣＰＵ２２によって実行される。その結果、エージェントプログラム１０の処理手順に従って、末端メモリ２４に格納されている第２Ｃ

ＲＬファイル（更新前の内容は「ＣＲＬ１」である。）２６の内容は、エージェントプログラム１０が認証局のコンピュータ１２から持ち帰った最新のＣＲＬである「ＣＲＬ２」に更新される（図２のＳ７）。尚、図１の（Ｃ）においては、第２ＣＲＬファイル２６の内容が「ＣＲＬ１」から「ＣＲＬ２」に更新された状態を示す。このようにして、エージェントプログラム１０により認証局１２から末端エンティティ１４へＣＲＬが配布される。

【００６６】このように、第１の実施の形態のＣＲＬの配布方法によれば、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラム１０を用いる。その結果、アプリケーションシステムとＣＲＬの配布とを切り離すことができる。このため、アプリケーションシステムの設計をＣＲＬの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【００６７】［第２の実施の形態］次に、第２の実施の形態では、図３および図４を参照して、この発明の第２の無効ディジタル証明書リスト（ＣＲＬ）の配布方法の一例について説明する。

【００６８】図３の（Ａ）～（Ｃ）は、第２の実施の形態のＣＲＬの配布方法の説明に供するブロック図である。また、図４は、第１の実施の形態のＣＲＬの配布方法の説明に供するフローチャートである。

【００６９】また、通常は、認証局から多数の末端エンティティへＣＲＬが配布されるが、第２の実施の形態では、第１の実施の形態と同様に、１つの末端エンティティおよび認証局に注目してＣＲＬの配布方法について説明する。

【００７０】また、ＣＲＬを配布するための処理手順がプログラムされたエージェントプログラム（以下、単に「エージェント」とも称する。）３０が稼働する環境には、起動前のエージェント３０が認証局のコンピュータの認証局メモリにコンパイルさて格納されている点を除いては、上述した第１の実施の形態における環境と同一である。従って、図１に示された環境の成分と同一の環境の成分については図３において同一の符号を付し、その詳細な説明を省略する。

【００７１】次に、第２の実施の形態におけるＣＲＬの配布方法について説明する。

【００７２】ＣＲＬの配布を行うにあたり、先ず、認証局メモリ１８に格納されていたエージェントプログラム３０を認証局ＣＰＵ１６によって起動する（図４のＳ１）。すなわち、認証局ＣＰＵ１６によってエージェントプログラム３０の実行を開始する。起動にあたっては、例えば、認証局メモリ１８中に格納されているローカルな関数の呼び出しを認証局ＣＰＵ１６によって行うことによって、エージェント３０の実行を開始させると良い。

【００７３】次に、認証局ＣＰＵ１６によってエージェントプログラム３０を実行することにより、認証局メモリ１８のうちのこのエージェントプログラム３０が使用するメモリ領域に、認証局の発行している最新の無効ディジタル証明書リスト（ＣＲＬ）が格納される（図４のＳ２）。ここでは、第１ＣＲＬファイル２０からメモリ領域のＣＲＬ読込みファイル３０ａに、最新ＣＲＬとして「ＣＲＬ２」を読み込む（図３の（Ａ））。図３の（Ａ）においては、エージェント３０のＣＲＬ読込みファイル３０ａに、「ＣＲＬ２」が読み込まれた状態を示す。

【００７４】次に、認証局ＣＰＵ１６によってエージェントプログラム３０を実行することにより、エージェントプログラム３０自身を、ＣＲＬ読込みファイル３０ａに格納された最新のＣＲＬ（「ＣＲＬ２」）と共に、末端エンティティ１４へオープンネットワークシステムを介して送って、末端メモリ（ＥＥメモリ）２４に格納する（図４のＳ３）。すなわち、エージェントプログラム３０は、自身のプログラムに従って、末端エンティティ１４へ移動する（図３の（Ｂ））。

【００７５】次に、末端メモリ２４に格納されたエージェントプログラム３０は、末端ＣＰＵ２２によって実行される。その結果、エージェントプログラム３０の処理手順に従って、当該末端メモリ２４に格納されている第２ＣＲＬファイル２６の内容が、ＣＲＬ読込みファイル３０ａの内容に更新される（図４のＳ４）。ここでは、第２ＣＲＬファイル２６の内容「ＣＲＬ１」から「ＣＲＬ２」に更新する。このようにして、エージェントプログラム３０により認証局から末端エンティティへ最新のＣＲＬが配布される（図３の（Ｂ））。

【００７６】尚、図３の（Ｂ）においては、第２ＣＲＬファイル２６の内容が、「ＣＲＬ１」から「ＣＲＬ２」に更新された状態を示す。また、図４において、太線の枠で示したＳ４およびＳ５のステップの処理は、末端ＣＰＵ２２がエージェントプログラム３０を実行することによって行われる。また、Ｓ４およびＳ５のステップ以外の処理（細線の枠で示されたステップＳ１～Ｓ３およびＳ５）の処理は、認証局ＣＰＵ１６がエージェントプログラム３０を実行することによって行われる。

【００７７】次に、エージェントプログラム３０は、認証局ＣＰＵ１６によってエージェントプログラム３０が実行されることにより、認証局メモリ（ＣＡメモリ）１８に、オープンネットワークシステムを介して送られて格納される（図４のＳ５）。すなわち、エージェントプログラムは、自身のプログラムに従って、認証局メモリ１８に移動する（図３の（Ｃ））。

【００７８】そして、認証局に戻ったエージェントプログラム３０は、認証局ＣＰＵ１６に対して、ＣＲＬの配布が完了したことを報告する。

【００７９】尚、第２の実施の形態においては、１つの

末端エンティティへＣＲＬを配布する例について説明したが、この発明の第２のＣＲＬの配布方法では、複数の末端エンティティへＣＲＬを配布することも十分可能である。

【００８０】その場合、例えば１つのエージェントが、１つの末端エンティティへＣＲＬを配布した後、認証局へ戻らずに、複数の末端エンティティへＣＲＬを順次に配布し、最後に認証局に戻っても良い。すなわち、図４に示したフローチャートにおいて、Ｓ３およびＳ４のステップを繰返しても良い。

【００８１】そして、エージェントが複数の末端エンティティに順次にＣＲＬを配布した場合には、認証局への完了報告に、例えば、実際にＣＲＬを配布した末端エンティティの一覧を含めると良い。そして、認証局ＣＰＵに、末端エンティティの一覧に含まれていない末端エンティティ、すなわち、接続不能や末端メモリの容量不足のためにＣＲＬの配布ができなかった末端エンティティを認証局ＣＰＵに把握させても良い。さらに、ＣＲＬの配布ができなかった末端エンティティに対してだけ、再びＣＲＬの配布を試みても良い。

【００８２】また、この発明の第２のＣＲＬの配布方法によれば、例えば、複数のエージェントを同時に実行させても良い。

【００８３】このように、第２の実施の形態のＣＲＬの配布方法によれば、エージェントプログラム３０を用いる。そして、このエージェントプログラム３０にＣＲＬの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をＣＲＬの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【００８４】さらに、第２の実施の形態のＣＲＬの配布方法によれば、認証局ＣＰＵ１６によって、エージェントプログラム３０を起動して、エージェントプログラム３０を末端メモリ２４へ移動させる。その結果、多数の末端エンティティへＣＲＬを配布する場合でも、認証局１２へ末端エンティティからエージェントプログラムが殺到することがない。このため、認証局のコンピュータ１２の負担の増大を抑制することができる。よって、特に認証局のコンピュータ１２の処理能力に余裕がない場合に適用して好適である。

【００８５】［第３の実施の形態］第３の実施の形態では、図５、図６および図７を参照して、この発明の第３の無効ディジタル証明書リスト（ＣＲＬ）の配布方法の一例について説明する。

【００８６】図５の（Ａ）～（Ｃ）および図６の（Ａ）～（Ｃ）は、第３の実施の形態のＣＲＬの配布方法の説明に供するブロック図である。また、図７は、第３の実施の形態のＣＲＬの配布方法の説明に供するフローチャートである。

【００８７】先ず、１つの認証局から他の認証局へＣＲＬを配布するための処理手順がプログラムされたエージェントプログラム（以下、単に「エージェント」とも称する。）が稼働する環境について説明する。通常は、多数の認証局どうしの間でＣＲＬが互いに配布されるが、ここでは、第１認証局および第２認証局に注目してＣＲＬの配布方法について説明する。

【００８８】図５および図６には、第１認証局のコンピュータ（「第１ＣＡコンピュータ」または「第１認証局」とも称する。）３２と、第２認証局のコンピュータ（「第２ＣＡコンピュータ」または「第２認証局」とも表記する。）３４を示す。第１認証局３２と第２認証局３４とは、互いにオープンネットワークシステムよって接続してある。また、第１認証局３２および第２認証局３４は、いずれも、第１認証局３２の発行するＣＲＬを配布する第１エージェント３６および第２認証局３４の発行するＣＲＬを配布する第２エージェント３８が動作可能な環境を有している。動作可能な環境とは、例えば、第１認証局３２と第２認証局３４との間で第１および第２エージェント３６および３８のそれぞれの受渡が可能な状態をいう。

【００８９】また、第１認証局３２は、第１認証局ＣＰＵ４０および第１認証局メモリ４２を具えている。この第１認証局メモリ４２には、この第１認証局のコンピュータ３２が発行した最新の無効ディジタル証明書リスト（ＣＲＬ）を内容とする第１ＣＲＬファイル４４が格納されている。図５の（Ａ）においては、第１ＣＲＬファイル４４に、最新のＣＲＬとして「ＣＲＬ２」が格納された状態を示す。

【００９０】また、この第１認証局メモリ４２には、第２認証局のコンピュータ３４から配布されたＣＲＬを内容とする第２ＣＲＬファイル４６が格納されている。また、図５の（Ａ）においては、この実施の形態におけるＣＲＬの配布前の状態として、第２ＣＲＬファイル４６に「ＣＲＬ３」が格納されている状態を示す。

【００９１】そして、第１認証局メモリ４２には、第１エージェントプログラム３６がコンパイルされた状態で格納してある（図５の（Ａ））。尚、図６の（Ａ）～（Ｃ）では、第１エージェントプログラム３６の図示を省略する。

【００９２】また、第２認証局３４は、第２認証局ＣＰＵ４８および第２認証局メモリ５０を具えている。この第２認証局メモリ５０には、この第２認証局のコンピュータ３４が発行した最新のＣＲＬを内容とする第３ＣＲＬファイル５２が格納されている。第３の実施の形態においては、第３ＣＲＬファイル５２に最新のＣＲＬとして「ＣＲＬ４」が格納されている。

【００９３】また、この第２認証局メモリ５０には、第１認証局のコンピュータ３２から配布されたＣＲＬを内容とする第４ＣＲＬファイル５４が格納されている。図

５の（Ａ）においては、この実施の形態で説明するＣＲＬの配布前の状態として、第４ＣＲＬファイル５４に「ＣＲＬ１」が格納されている状態を示す。

【００９４】そして、第２認証局メモリ５０には、第２エージェントプログラム３８がコンパイルされた状態で格納してある。尚、図５の（Ａ）～（Ｃ）では、第２エージェントプログラム３８の図示を省略してある。

【００９５】次に、第３の実施の形態におけるＣＲＬの配布方法について説明する。ここでは、第１認証局のコンピュータ３２から第２認証局のコンピュータ３４へＣＲＬを配布した後、第２認証局のコンピュータ３４から第１認証局のコンピュータ３２へＣＲＬを配布する例について説明する。

【００９６】先ず、第１認証局３２から第２認証局３４へのＣＲＬの配布を行うにあたり、第１認証局メモリ４２に格納されていた第１エージェントプログラム３６を第１認証局ＣＰＵ４０によって起動する（図７のＳ１）。すなわち、第１認証局ＣＰＵ４０によって第１エージェントプログラム３６の実行を開始する。起動にあたっては、例えば、第１認証局メモリ４２中に格納されているローカルな関数の呼び出しを第１認証局ＣＰＵ４０によって行うことによって、第１エージェントプログラム３６の実行を開始させると良い。

【００９７】次に、第１認証局ＣＰＵ４０によって第１エージェントプログラム３６を実行することにより、認証局メモリ４２のうちのこの第１エージェントプログラム３６が使用するメモリ領域に、第１認証局の発行している最新の無効ディジタル証明書リスト（ＣＲＬ）を格納する（図７のＳ２）。ここでは、このメモリ領域のＣＲＬ読込みファイル３６ａに、第１ＣＲＬファイル４４から最新ＣＲＬとして「ＣＲＬ２」を読み込む（図５の（Ａ））。図５の（Ａ）においては、ＣＲＬ読込みファイル３６ａに、「ＣＲＬ２」が読み込まれた状態を示す。

【００９８】次に、第１認証局ＣＰＵ４０によって第１エージェントプログラム３６を実行することにより、第１エージェントプログラム３６自身を、ＣＲＬ読込みファイル３６ａに格納された最新のＣＲＬである「ＣＲＬ２」と共に、第２認証局３４へオープンネットワークシステムを介して送って、第２認証局メモリ５０に格納する（図５の（Ｂ））。すなわち、第１エージェントプログラム３６は、自身のプログラムに従って、第２認証局（第２ＣＡ）３４へ移動する（図７のＳ３）。

【００９９】次に、第２認証局メモリ５０に格納された第１エージェントプログラム３６は、第２認証局ＣＰＵ４８によって実行される。その結果、第１エージェントプログラム３６の処理手順に従って、第２認証局メモリ５０の第４ＣＲＬファイル５４に格納されている古いＣＲＬ（ここでは「ＣＲＬ１」）が、最新のＣＲＬ（「ＣＲＬ２」）に更新される（図７のＳ４）。このようにして、第１エージェントプログラム３６によって第１認証局３２から第２認証局３４へ最新のＣＲＬ（「ＣＲＬ２」）が配布される（図５の（Ｂ））。

【０１００】尚、図５の（Ｂ）においては、第４ＣＲＬファイル５４の内容が「ＣＲＬ２」に更新される前の状態を示す。また、図７において細線の枠で示したＳ１～Ｓ３のステップの処理は、前述したように、第１認証局ＣＰＵ４０が第１エージェントプログラム３６を実行することによって行われる。これに対して、太線の枠で示したＳ４～Ｓ５のステップの処理は、第２認証局ＣＰＵ４８が第１エージェントプログラム３６を実行することによって行われる。また、図７において太線の枠で示したＳ６～Ｓ８のステップの処理は、第２認証局ＣＰＵ４８が第２エージェントプログラム３８を実行することによって行われる。これに対して、細線の枠で示されたＳ９およびＳ１０のステップの処理は、第１認証局ＣＰＵ４０が第２エージェントプログラム３８を実行することによって行われる。

【０１０１】次に、第１エージェントプログラム３６は、第２認証局ＣＰＵ４８によって第１エージェントプログラム３６が実行されることにより、第１認証局３２にオープンネットワークシステムを介して送られて、第１認証局メモリ４２格納される（図５の（Ｃ））。すなわち、エージェントプログラム３６は、自身のプログラムに従って、第１認証局（第１ＣＡ）３２に移動する（図７のＳ５）。

【０１０２】そして、第１認証局３２に戻った第１エージェントプログラム３６は、第１認証局ＣＰＵ４０に対して、ＣＲＬの配布が完了したことを報告する。

【０１０３】次に、第２認証局３４から第１認証局３２へのＣＲＬの配布を行うにあたり、第２認証局メモリ５０に格納されていた第２エージェントプログラム３８を第２認証局ＣＰＵ４８によって起動する（図７のＳ６）。すなわち、第２認証局ＣＰＵ４８によって第２エージェントプログラム３８の実行を開始する。起動にあたっては、例えば、第２認証局メモリ５０中に格納されているローカルな関数の呼び出しを第２認証局ＣＰＵ４８によって行うことによって、第２エージェントプログラム３８の実行を開始させると良い。

【０１０４】次に、第２認証局ＣＰＵ４８によって第２エージェントプログラム３８を実行することにより、第２認証局メモリ５０のうちのこの第２エージェントプログラム３８が使用するメモリ領域に、第２認証局３４の発行している最新の無効ディジタル証明書リスト（ＣＲＬ）を格納する（図７のＳ７）。ここでは、このメモリ領域のＣＲＬ読込みファイル３８ａに、第３ＣＲＬファイル５２から最新ＣＲＬとして「ＣＲＬ４」を読み込む（図６の（Ａ））。図６の（Ａ）においては、ＣＲＬ読込みファイル３８ａに、「ＣＲＬ４」が読み込まれた状態を示す。

【0105】次に、第2認証局CPU48によって第2エージェントプログラム38を実行することにより、第2エージェントプログラム38自身を、CRL読込みファイル36aに格納された最新のCRLである「CRL4」と共に、第1認証局32へオープンネットワークシステムを介して送って、第1認証局メモリ42に格納する（図6の（B））。即ち、第2エージェントプログラム38は、自身のプログラムに従って、第1認証局（第1CA）32へ移動する（図7のS8）。

【0106】次に、第1認証局メモリ42に格納された第2エージェントプログラム38は、第1認証局CPU40によって実行される。その結果、第2エージェントプログラム38の処理手順に従って、第1認証局メモリ42の第2CRLファイル46に格納されている古いCRL（ここでは「CRL3」）が、最新のCRL（「CRL4」）に更新される（図7のS9）。このようにして、第2エージェントプログラム38によって第2認証局34から第1認証局32へ最新のCRL（「CRL4」）が配布される（図6の（B））。尚、図6の（B）においては、第2CRLファイル46の内容が「CRL4」に更新される前の状態を示す。

【0107】次に、第2エージェントプログラム38は、第1認証局CPU40によって第2エージェントプログラム38が実行されることにより、第2認証局34にオープンネットワークシステムを介して送られて、第2認証局メモリ50格納される（図6の（C））。すなわち、エージェントプログラム36は、自身のプログラムに従って、第2認証局（第2CA）34に移動する（図7のS10）。

【0108】そして、第2認証局34に戻った第2エージェントプログラム38は、第2認証局CPU48に対して、CRLの配布が完了したことを報告する。

【0109】このように、第3の実施の形態の無効ディジタル証明書リストの配布方法によれば、第1および第2エージェントプログラム36および38を用いる。そして、この第1および第2エージェントプログラム36および38のそれぞれにCRLの配布の仕組みの処理手順を設計する。その結果、個々の認証局32および34のシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、第1および第2認証局32および34のシステムの設計の負担を軽減することができる。

【0110】また、第3の実施の形態においては、第1認証局32と第2認証局34との間でCRLを配布する場合について説明したが、この発明の第3のCRLの配布方法によれば、3つ以上の認証局どうしの間でCRLを互いに配布することも可能である。

【0111】また、第3の実施の形態においては、第1認証局から第2認証局へCRLを配布した後に、第2認証局から第1認証局へCRLを配布したが、この発明の第3のCRLの配布方法では、CRLの配布の順序は限定されない。例えば、第1認証局と第2認証局との間のCRLの配布を同時に行っても良い。より具体的には、例えば、図7に示す各ステップをS1、S6、S2、S7、S3、S8、S9、S10の順序で実行しても良い。

【0112】

【発明の効果】

[第1の無効ディジタル証明書リストの配布方法について] この発明の第1の無効ディジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにCRLの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【0113】また、この発明の第1の無効ディジタル証明書リストの配布方法を実施するにあたり、エージェントを認証局に駐在させる一定時間を設定して末端メモリに格納しておき、これをエージェントプログラムに読み込ませて設定すれば、エージェントプログラムが認証局に駐在している時間の長さを所望の長さとすることができる。その結果、エージェントプログラムが認証局から末端エンティティに戻ってくるタイミングを所望のタイミングとすることができる。このため、CRLの更新のタイミングを所望のタイミングとすることができる。

【0114】[第2の無効ディジタル証明書リストの配布方法について] また、この発明の第2の無効ディジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにCRLの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【0115】さらに、この発明の第2の無効ディジタル証明書リストの配布方法によれば、認証局CPUによって、エージェントプログラムを起動して、エージェントプログラムを末端メモリへ移動させる。このため、第2の無効ディジタル証明書リストの配布方法によれば、認証局へ末端エンティティからエージェントプログラムが殺到することがない。その結果、認証局のコンピュータの負担の増大を抑制することができる。従って、第2の無効ディジタル証明書リストの配布方法は、特に認証局のコンピュータの処理能力に余裕がない場合に適用して好適である。

【0116】[第3の無効ディジタル証明書リストの配布方法について] また、この発明の第3の無効ディジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラム

にＣＲＬの配布の仕組みの処理手順を設計する。その結果、個々の認証局のシステムの設計をＣＲＬの配布の仕組みの設計から切り離して行うことができる。このため、認証局のシステムの設計の負担を軽減することができる。

【図面の簡単な説明】

【図１】第１の実施の形態の無効ディジタル証明書リストの配布方法の説明に供するブロック図である。

【図２】第１の実施の形態の無効ディジタル証明書リストの配布方法の説明に供するフローチャートである。

【図３】第２の実施の形態の無効ディジタル証明書リストの配布方法の説明に供するブロック図である。

【図４】第２の実施の形態の無効ディジタル証明書リストの配布方法の説明に供するフローチャートである。

【図５】第３の実施の形態の無効ディジタル証明書リストの配布方法の説明に供する前半のブロック図である。

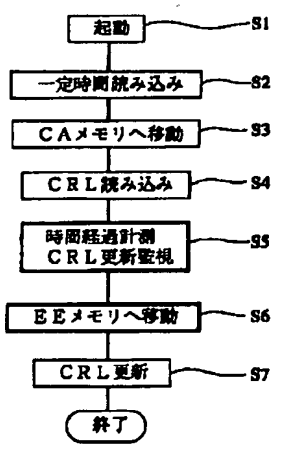
【図６】第３の実施の形態の無効ディジタル証明書リストの配布方法の説明に供する後半のブロック図である。

【図７】第３の実施の形態の無効ディジタル証明書リストの配布方法の説明に供するフローチャートである。

【符号の説明】

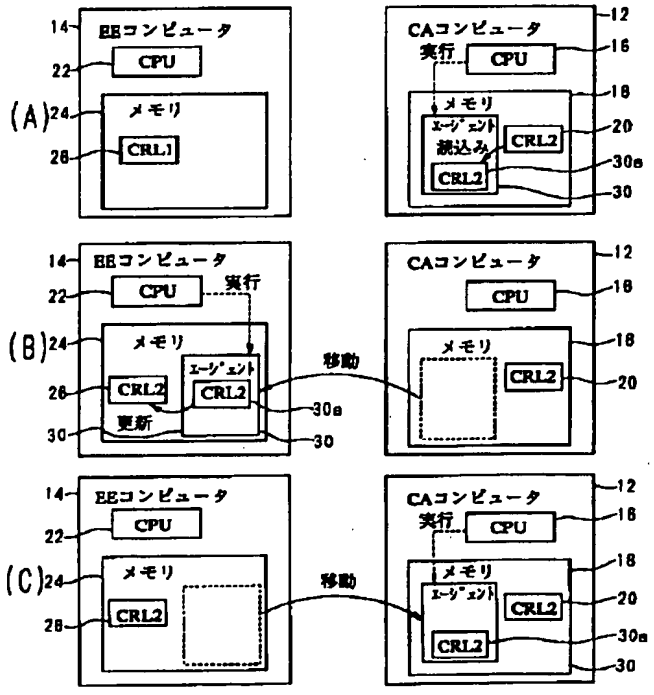
１０：エージェントプログラム
１０ａ：ＣＲＬ読込みファイル
１２：認証局のコンピュータ（認証局）
１４：末端エンティティのコンピュータ（末端エンティティ）
１６：認証局ＣＰＵ
１８：認証局メモリ
２０：第１ＣＲＬファイル
２２：末端ＣＰＵ
２４：末端メモリ
２６：第２ＣＲＬファイル
２８：一定時間を設定したファイル
３０：エージェントプログラム
３０ａ：ＣＲＬ読込みファイル
３２：第１認証局のコンピュータ（第１認証局）
３４：第２認証局のコンピュータ（第２認証局）
３６：第１エージェントプログラム
３６ａ：ＣＲＬ読込みファイル
３８：第２エージェントプログラム
３８ａ：ＣＲＬ読込みファイル
４０：第１認証局ＣＰＵ
４２：第１認証局メモリ
４４：第１ＣＲＬファイル
４６：第２ＣＲＬファイル
４８：第２認証局ＣＰＵ
５０：第２認証局メモリ
５２：第３ＣＲＬファイル
５４：第４ＣＲＬファイル

【図２】



第１の実施の形態のフローチャート

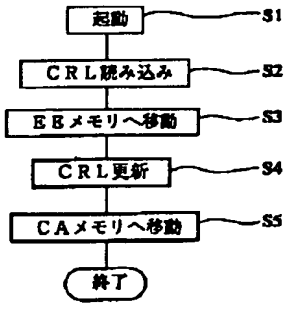
【図３】



30：エージェントプログラム　　30a：ＣＲＬ読込みファイル

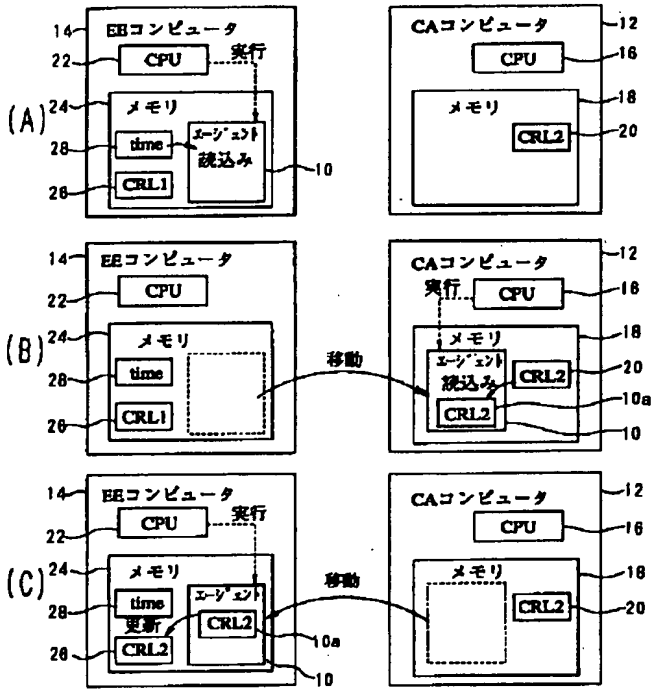
第２の実施の形態のブロック図

【図４】



第２の実施の形態のフローチャート

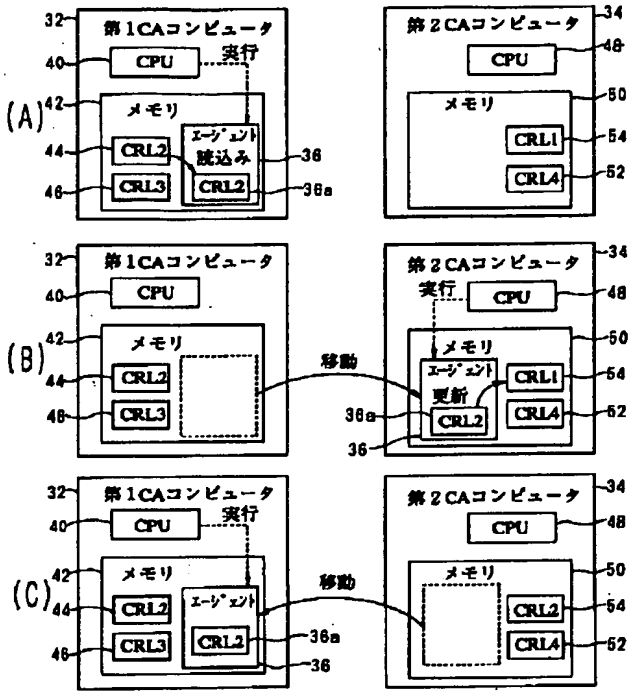
【図1】



10：エージェントプログラム　10a：ＣＲＬ読込みファイル
12：認証局のコンピュータ　14：末端エンティティのコンピュータ
16：認証局ＣＰＵ　18：認証局メモリ
20：第１ＣＲＬファイル　22：末端ＣＰＵ
24：末端メモリ　28：第２ＣＲＬファイル
26：一定時間を設定したファイル

第１の実施の形態のブロック図

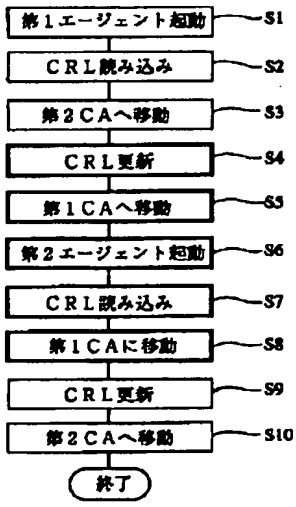
【図5】



32：第１認証局のコンピュータ　34：第２認証局のコンピュータ
36：第１エージェントプログラム　36a：ＣＲＬ読込みファイル
40：第１認証局ＣＰＵ　42：第１認証局メモリ
44：第１ＣＲＬファイル　48：第２ＣＲＬファイル
46：第２認証局ＣＰＵ　50：第２認証局メモリ
52：第３ＣＲＬファイル　54：第４ＣＲＬファイル

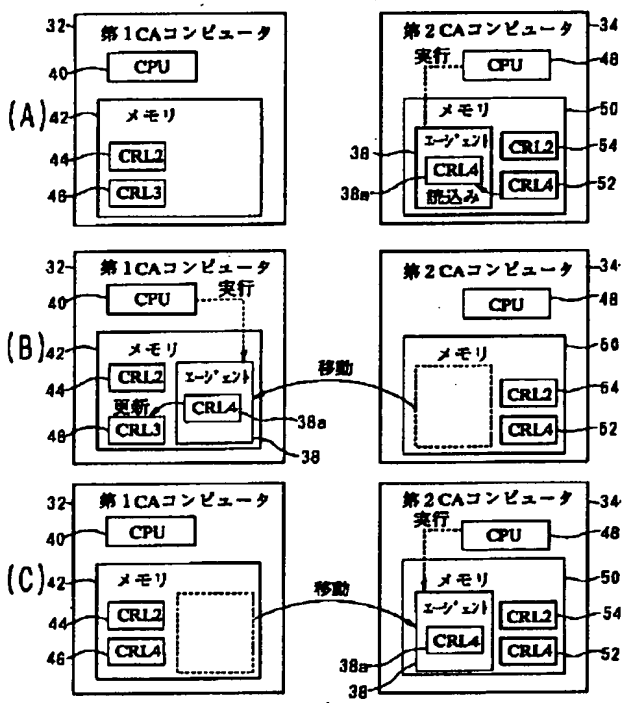
第３の実施の形態のブロック図（前半）

【図7】



第３の実施の形態のフローチャート

【図６】



38：第２エージェントプログラム　　38a：ＣＲＬ読込みファイル

第３の実施の形態のブロック図（後半）